Safeguard your SEA- cret data

The internet is full of choppy waters — learn how to navigate your inbox safely.

Phishing is what everyone is always talking about and for good reason. Phishing is the leading cause of cyberattacks. According to The Psychology of Human Error, research by Tessian, nearly half of employees are "very" or "pretty" certain they have made a workplace mistake with security repercussions. This is alarming and very dangerous.

Research shows that the most clicked phishing emails come from ones that are disguised as corporate communications, such as emails about performance reviews and approval of documents. These phishy emails have an average click rate of 10-20%! While most internal emails are safe, hackers use email spoofing to make the email address look like it is being sent from an internal or trusted source, but it's a phishing email.

To avoid falling for a phishing email that looks like it is from your organization, go straight to the official source to authenticate or view whatever you are asked to see in the email. For example, if it looks like an email from Human Resources, go to your organization's Human Resources page to view the information and avoid the link in the email.

Here are a few specific examples of phishing attacks to familiarize yourself with:

Float safely around Spearphishing attacks

A Spear phishing attack is often subtle: hackers send emails linking to fake login pages, designed to harvest your credentials. They disguise their messages as requests or orders from employers. Spearphishing attacks are more likely to target people accessing data, systems or restricted areas.

It's a phish, it's a shark, no it's a Whaling attack!

Whaling is phishing for a large target: i.e., an individual within the target organization who holds much power. Attackers specifically phish executives, CEOs, accounting departments, heads of security and other people with high-level access. If a hacker compromises their account, the entire company could suffer huge losses, even going bankrupt.

One Phish Two Phish Clone Phish Attack

Clone phishing is a highly dangerous form of phishing. It duplicates messages from trusted individuals, groups, or brands. for instance, a phishing email might contain a link to a realistic-looking login page for a popular online store or social media platform. It could disguise itself as a software update or a delivery notification. Many clone phishing emails copy messages from individuals you trust.

Avoid PIER pressure from Business Email Compromise (BEC) attacks

In a BEC attack, the hacker pretends to be a professional contact. This could be your boss, the CEO, an attorney, or an outside vendor. The hacker creates an email that copies a real person's writing style and quirks. The result is a personalized email that looks completely legitimate. The attacker then asks you to pay a phony invoice or send them some classified company documents. And since the email looks legitimate, you are far more likely to do it. Anyone with access to confidential data or company finances may be a target of BEC. Typical targets include CFOs, Human Resources and upper-management positions.

Cybersecurity roles — Cyber Defense Analyst

Have you ever wondered what your friendly cybersecurity team is up to? We'll share a cybersecurity job role each month to give you an inside look!

Cyber Defense Analyst
Cyber Defense Analysts use data collected from various cyber defense tools such as Wireshark for continual monitoring and analysis of systems to identify malicious activity. As they analyze their organization's systems, they are working diligently to mitigate any threats that may come their way. They stay on top of trends, research and reporting to protect their critical systems.

E-TECH